UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/816,883	03/23/2001	Michael J. Badamo	70066	6901

23872 7590 08/11/2004

MCGLEW & TUTTLE, PC
1 SCARBOROUGH STATION PLAZA
SCARBOROUGH, NY 10510-0827

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	7

DATE MAILED: 08/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/816,883	BADAMO ET AL.	
	Examiner	Art Unit	
	Beemnet W Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 have been examined.

Claim Objections

2. Claim 5 is objected to because of the following informalities: the sentence "said ingress ... decryption algorithm" is repeated. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 20 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Ellington, Jr. et al (hereinafter Ellington) (US Patent No. 6,708,218 B1).

5. As per claim 20, Ellington teaches a process for secure communication between network entities, the process comprising the steps of:

providing a device with a network interface and physical connection with a packet processing system (i.e., data arrival endpoint in the gateway) including an ingress processing subsystem and an egress processing subsystem (i.e., data forwarding endpoint in the gateway) [column 4, lines 45-64 and figure 1];

making a key exchange between the network entity and the other network entity and hosting a security association upon completion of the key exchange in association with a processing entity of the packet processing system, the security association including information as to authentication, encryption and changing of keys (gateway-to-gateway IPSec and IKE) [column 4, lines 64-67, column 5, lines 1-21 and figure 2];

extracting data derived from the security association [column 8, lines 59-67 and column 9, lines 1-9];

sending a message from a processing entity hosting the security association to one or both of said ingress processing subsystem and said egress processing subsystem to provide a security association at the processing subsystems [column 8, lines 59-67 and column 9, lines 1-23].

6. As per claim 21, Ellington teaches the process as applied above. Furthermore, Ellington teaches the process wherein said packet processor includes an ingress processing security subsystem and an egress processing security subsystem and a processor subsystem for handling key exchanges and for distributing SAs to the ingress processing security subsystem and said egress processing security subsystem [column 9, lines 1-9 and figure 9 unit 94].

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-19 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellington (US Patent No. 6,708,218 B1) in view of Ylonen et al. (hereinafter Ylonen) (US Patent No. 6,438,612 B1).

9. As per claim 1, Ellington teaches a network device comprising:

a network physical interface for receiving and transmitting data and for receiving packets for transmission and forwarding packets from received data [column 4, lines 45-64 and figure 1]; and

a packet processor hosting a security association (SA) used for encryption and decryption for communication with a network peer and including [column 8, lines 59-67, column 9, lines 1-9 and figure 9 unit 94]:

an ingress processing security subsystem (i.e., data arrival endpoint in the gateway) with a decryption processor for decrypting packets [column 6, lines 65-67 and column 7, lines 1-22]; and

an egress processing security subsystem (i.e., data forwarding endpoint in the gateway) for encrypting packets [column 3, lines 23-27 and column 7, lines 1-25]. Ellington does not clearly teaches one or both of said ingress processing security subsystem and said egress processing security subsystem receiving both of ingress and egress security associations. However, Ylonen teaches a method of secure data transmission between virtual routers (i.e. a secure gateway) wherein an ingress processing security subsystem (i.e., data arrival endpoint in the gateway) and egress processing security subsystem (i.e., data forwarding endpoint in the gateway) receiving both of ingress and egress security associations [column 5, lines 55-67,

column 6, lines 1-14, 57-67 and column 7, lines 1-15]. Therefore it would have been obvious to a person with ordinary skill in the art at the time the invention was made to incorporate the method of receiving both of ingress and egress security in both of ingress and egress processing subsystems as taught by Ylonen into the secure gateway device of Ellington in order to enhance the security mechanism in virtual routers by enabling the identification of virtual routers in the course of tunneling data packets through network.

10. As per claim 2, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches the device wherein said packet processor includes a processor subsystem for handling key exchanges and for distributing SAs to the ingress processing security subsystem and said egress processing security subsystem [column 9, lines 1-9 and figure 9 unit 94].

11. As per claim 3, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ylonen teaches the device wherein said ingress processing security subsystem and said egress processing security subsystem hosts a security association (SA) used for encryption and decryption for communication with a network peer and one of said ingress processing security subsystem and said egress processing security subsystem distributing at least one of ingress and egress SAs to the other of said ingress processing security subsystem and said egress processing security subsystem [column 5, lines 55-67, column 6, lines 1-14, 57-67 and column 7, lines 1-15].

12. As per claim 4, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches the device wherein said packet processor includes an

ingress processor system for ingress processing of received packets and an egress processor system for processing packets for transmission [column 6, lines 65-67 and column 7, lines 1-22].

13. As per claim 5, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches the device wherein said ingress processing security subsystem includes decryption means for running decryption algorithm [column 6, lines 65-67 and column 7, lines 1-22].

14. As per claim 6, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches the device further comprising a packet queue establishing a queue of packets awaiting transmission, said packet queue being the exclusive buffer for packets between packets entering [column 7, lines 1-28],

15. As per claims 7, 9, 11 and 13, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches the device, wherein packets exit the device at a rate of the line established at the physical interface or processing packets at speed greater than or equal to the rate at which they enter the device [column 7, lines 1-28].

16. As per claim 8, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches the device wherein said ingress processing system processes packets including at least one or more of protocol translation, de-encapsulation, decryption, authentication, point-to-point protocol (PPP) termination and network address translation (NAT), and said egress processing system processes packets including at least one

or more of protocol translation, encapsulation, encryption, generation of authentication data, PPP generation and NAT [column 5, lines 1-11 and column 6, lines 1-19].

17. As per claim 10, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches converting packets from one protocol to another [column 7, lines 1-14].

18. As per claim 12, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches processing NAT [column 5, lines 44-56].

19. As per claims 14 and 16, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ylonen teaches the device wherein said physical interface includes a line card and said ingress processor system is provided as part of a service card and said egress processor system is provided in one of said service card and another service card and said interconnections include: a line card bus connected to said line card; a service card bus connected to at least one of said service card and said another service card; and a switch fabric connecting said line card to at least one of said service card and said another service card [column 5, lines 39-55 and figure 3].

20. As per claims15 and 19, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ellington teaches the device wherein said ingress processing security subsystem includes decryption means for running decryption algorithm [column 6, lines 65-67 and column 7, lines 1-22].

21. As per claim 17, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ylonen teaches the device wherein said physical interface includes another line card connected by said switch fabric to at least one of said service card and said another service card [column 5, lines 39-55 and figure 3].

22. As per claim 18, the combination of Ellington and Ylonen teaches the device as applied above. Furthermore, Ylonen teaches the device wherein said switch fabric connects any one of said line cards to any one of said service cards, whereby any line card can send packet traffic to any service card and routing of packet traffic is configured one of statically and dynamically by the said line card [column 5, lines 39-55 and figure 3].

23. As per claim 22, Ellington teaches the process as applied to claim 20 above. Ellington does not clearly teach one or both of said ingress processing security subsystem and said egress processing security subsystem receiving both of ingress and egress security associations. However, Ylonen teaches a method of secure data transmission between virtual routers (i.e. a secure gateway) wherein an ingress processing security subsystem (i.e., data arrival endpoint in the gateway) and egress processing security subsystem (i.e., data forwarding endpoint in the gateway) receiving both of ingress and egress security associations as a security message [column 5, lines 55-67, column 6, lines 1-14, 57-67 and column 7, lines 1-15]. Therefore it would have been obvious to a person with ordinary skill in the art at the time the invention was made to incorporate the method of receiving both of ingress and egress security in both of ingress and egress processing subsystems as taught by Ylonen into the secure gateway device of Ellington in order to enhance the security mechanism in virtual routers by enabling the identification of virtual routers in the course of tunneling data packets.

24. As per claim 23, the combination of Ellington and Ylonen teaches the process as applied above. Furthermore, Ellington teaches the process further comprising: selecting either the ingress processing subsystem or the egress processing subsystem to host a security association [column 9, lines 1-9 and figure 9 unit 94].

25. As per claim 24, the combination of Ellington and Ylonen teaches the method as applied above. Furthermore, Ellington teaches the process wherein said security message includes authentication features for authenticating the transmission of said session data [column 7, lines 15-28].

26. As per claim 25, the combination of Ellington and Ylonen teaches the method as applied above. Furthermore, Ellington teaches the process further comprising the steps of establishing a shared secret key at each of the ingress processor and egress processor for use for symmetric block encryption; and encrypting said session data using the symmetric block encryption cipher [column 7, lines 15-28].

Claim Rejections - 35 USC § 102

27. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

28. Claims 20 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Kunzinger (US Pub No. 2002/0091921 A1).

29. As per claim 20, Kunzinger teaches a process for secure communication between network entities, the process comprising the steps of:

providing a device with a network interface and physical connection with a packet (datagram) processing system (i.e., data arrival endpoint in the gateway) including an ingress processing subsystem and an egress processing subsystem (i.e., data forwarding endpoint in the gateway) [page 5, 0056, page 6, 0066 and figure 9];

making a key exchange between the network entity (i.e., client) and the other network entity (i.e., server) and hosting a security association upon completion of the key exchange in association with a processing entity of the packet processing system, the security association including information as to authentication, encryption and changing of keys (IPSec and IKE) [page 6, 0067];

extracting data derived from the security association (providing encryption/decryption key from SA) [page 6, 0068];

sending a message from a processing entity hosting the security association to one or both of said ingress processing subsystem and said egress processing subsystem to provide a security association at the processing subsystems [page 5, 0066 and page 6, 0068].

30. As per claim 21, Kunzinger teaches the process as applied above. Furthermore, Kunzinger teaches the process wherein said packet processor includes an ingress processing security subsystem and an egress processing security subsystem and a processor subsystem for handling key exchanges and for distributing SAs to the ingress processing security subsystem and said egress processing security subsystem [page 5, 0066 and page 6, 0068].

Claim Rejections - 35 USC § 103

31. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

32. Claims 1-5, 8, 14-19 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger (US Pub No. 2002/0091921 A1) in view of Ylonen et al. (hereinafter Ylonen) (US Patent No. 6,438,612 B1).

33. As per claim 1, Kunzinger teaches a network device comprising:

a network physical interface for receiving and transmitting data and for receiving packets for transmission and forwarding packets from received data [page 6, 0059-0065]; and

a packet processor hosting a security association (SA) used for encryption and decryption for communication with a network peer and including [page 6, 0066]:

an ingress processing security subsystem (i.e., data arrival endpoint in the gateway) with a decryption processor for decrypting packets [page 6, 0066 and 0068]; and

an egress processing security subsystem (i.e., data forwarding endpoint in the gateway) for encrypting packets [page 6, 0068, 0069].

Furthermore, Kunzinger teaches storing in the gateways egress and ingress SPDs (security policy database) key exchange and IPSec policy that is used to establish security associations. Kunzinger does not clearly teaches one or both of said ingress processing security subsystem and said egress processing security subsystem receiving both of ingress and egress security associations. However, Ylonen teaches a method of secure data transmission between virtual routers (i.e. a secure gateway) wherein an ingress processing security subsystem (i.e., data arrival endpoint in the gateway) and egress processing security subsystem (i.e., data forwarding endpoint in the gateway) receiving both of ingress and egress security associations [column 5, lines 55-67, column 6, lines 1-14, 57-67 and column 7, lines 1-15]. Therefore it would have been obvious to a person with ordinary skill in the art at the time the invention was made to incorporate the method of receiving both of ingress and egress security in both of ingress and egress processing subsystems as taught by Ylonen into the secure gateway device of Kunzinger in order to enhance the security mechanism in virtual routers by enabling the identification of virtual routers in the course of tunneling data packets through network.

34. As per claim 2, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said packet processor includes a processor subsystem for handling key exchanges and for distributing SAs to the ingress processing security subsystem and said egress processing security subsystem [page 6, 0066 and 0068].

35. As per claim 3, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said ingress processing security subsystem and said egress processing security subsystem hosts a security association (SA) used for encryption and decryption for communication with a network peer and one of said ingress processing security subsystem and said egress processing security subsystem distributing at least one of ingress and egress SAs to the other of said ingress processing security subsystem and said egress processing security subsystem [pages 5,6 0057, 0066, 0068].

36. As per claim 4, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said packet processor includes an ingress processor system for ingress processing of received packets and an egress processor system for processing packets for transmission, said ingress processor system including an ingress packet processor and including said ingress processing security subsystem, said egress processor system including an egress packet processor and including said egress processing security subsystem and interconnections including an interconnection between said ingress processor and said egress processor, an interconnection between said ingress processor and said physical interface and an interconnection between said ingress processor and said physical interface [page 6, 0066, 0068 and figure 9, 10].

37. As per claim 5, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said ingress processing security subsystem includes decryption means for running decryption algorithm [page 6, 0066 and 0068].

38. As per claim 8, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said ingress processing system processes packets including at least one or more of protocol translation, de-encapsulation, decryption, authentication, point-to-point protocol (PPP) termination and network address translation (NAT) [page 6, 0068] and said egress processing system processes packets including at least one or more of protocol translation, encapsulation, encryption, generation of authentication data, PPP generation and NAT [pages 6-7, 0069, 0071].

39. As per claim 14, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said physical interface includes a line card and said ingress processor system is provided as part of a service card and said egress processor system is provided in one of said service card and another service card and said interconnections include: a line card bus connected to said line card; a service card bus connected to at least one of said service card and said another service card; and a switch fabric connecting said line card to at least one of said service card and said another service card [page 3, 0037-0039].

40. As per claims 15 and 19, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said service card includes said ingress processor system and said egress processor system and said another service card includes another ingress processor system for processing all or part of packets received from said line card and for sending ingress processed packets for egress processing and another egress processor system for receiving ingress processed packets and for

processing all or part of received packets for sending to said line card, whereby packets may be sent between service cards for ingress processing by one service card and egress processing by another service card or for ingress processing using more than one service card [page 3, 0037-0039 and page 6, 0068].

41. As per claim 16, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein each of said service cards is identical and a spare service cards is provided, for functionally replacing any one of the other service cards to provide redundancy [page 6, 0066].

42. As per claim 17, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said physical interface includes another line card connected by said switch fabric to at least one of said service card and said another service card [page 3, 0037-0039].

43. As per claim 18, the combination of Kunzinger and Ylonen teaches the device as applied above. Furthermore, Kunzinger teaches the device wherein said switch fabric connects any one of said line cards to any one of said service cards, whereby any line card can send packet traffic to any service card and routing of packet traffic is configured one of statically and dynamically by the said line card [page 3, 0037-0039].

44. As per claim 22, Kunzinger teaches the process as applied to claim 20 above. Furthermore, Kunzinger teaches storing in the gateways egress and ingress SPDs (security policy database) key exchange and IPSec policy that is used to establish security associations.

Kunzinger does not clearly teaches one or both of said ingress processing security subsystem and said egress processing security subsystem receiving both of ingress and egress security associations. However, Ylonen teaches a method of secure data transmission between virtual routers (i.e. a secure gateway) wherein an ingress processing security subsystem (i.e., data arrival endpoint in the gateway) and egress processing security subsystem (i.e., data forwarding endpoint in the gateway) receiving both of ingress and egress security associations as a security message [column 5, lines 55-67, column 6, lines 1-14, 57-67 and column 7, lines 1-15]. Therefore it would have been obvious to a person with ordinary skill in the art at the time the invention was made to incorporate the method of receiving both of ingress and egress security in both of ingress and egress processing subsystems as taught by Ylonen into the secure gateway device of Kunzinger in order to enhance the security mechanism in virtual routers by enabling the identification of virtual routers in the course of tunneling data packets

45. As per claim 23, the combination of Kunzinger and Ylonen teaches the process as applied above. Furthermore, Kunzinger teaches the process further comprising: selecting either the ingress processing subsystem or the egress processing subsystem to host a security association [page 6, 0066].

46. As per claim 24, the combination of Kunzinger and Ylonen teaches the method as applied above. Furthermore, Kunzinger teaches the process wherein said security message includes authentication features for authenticating the transmission of said session data [page 7 0071].

47. As per claim 25, the combination of Kunzinger and Ylonen teaches the method as applied above. Furthermore, Kunzinger teaches the process further comprising the steps of establishing a shared secret key at each of the ingress processor and egress processor for use for symmetric block encryption; and encrypting said session data using the symmetric block encryption cipher [page 7, 0071].

48. Claims 6, 7 and 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kunzinger (US Pub No. 2002/0091921 A1) in view of Ylonen (US Patent No. 6,438,612 B1) to claim 4 above and further in view of Ellington, Jr. et al. (hereinafter Ellington) (US Patent No. 6,708,218 B1).

49. As per claim 6, the combination of Kunzinger and Ylonen teaches the gateway device as applied above. The combination of Kunzinger and Ylonen fails to teach a queue of packets establishing a queue of packets awaiting transmission, said packet queue being the exclusive buffer for packet transmission. However, queue of packets establishing a queue of packets awaiting transmission is well known in the art. For example, Ellington teaches a queue of packets establishing a queue of packets awaiting transmission, said packet queue being the exclusive buffer for packet transmission [column 7, lines 1-28], that has the benefit of transmitting and routing packets in first in first out protocol. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ a method of queue of packets awaiting transmission as taught by Ellington within the combination of Kunzinger and Ylonen in order to transmit / route packets in first in first out protocol.

50. As per claim 7, the combination of Kunzinger, Ylonen and Ellington teaches the gateway device as applied above. Furthermore, Ellington teaches the device wherein packets exit the device at a rate of the line established at the physical interface [column 6, lines 31-45].

51. As per claim 9, the combination of Kunzinger and Ylonen teaches the gateway device as applied above. The combination of Kunzinger and Ylonen fail to teach a fast path processor subsystem processing packets at a speed greater than or equal to the rate at which they enter the device. However Ellington teaches a fast path processor subsystem processing packets at a speed greater than or equal to the rate at which they enter the device [column 7, lines 40-55]. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ a method of fast path processor processing packets as per teachings of Ellington into the combination of Kunzinge and Ylonen in order to enhance the speed of data routing at the gate device.

52. As per claim 10, the combination of Kunzinger, Ylonen and Ellington teaches the device as applied above. Furthermore, Kunzinger teaches converting packets form one protocol to another [page 7, 0071].

53. As per claim 11, the combination of Kunzinger, Ylonen and Ellington teaches the device as applied above. Furthermore, Ellington teaches a fast path processor subsystem processing packets at a speed greater than or equal to the rate at which they enter the device [column 7, lines 40-55].

54. As per claim 12, the combination of Kunzinger, Ylonen and Ellington teaches the device as applied above. Furthermore, Kunzinger teaches processing NAT (network address translation) [page 5, 0050].

55. As per claim 13, the combination of Kunzinger, Ylonen and Ellington teaches the device as applied above. Furthermore, Ellington teaches processing packets concurrently with fast path processor packet processing [column 7, lines 40-55].

Conclusion

56. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Beemnet Dada

August 7, 2004